line 8, change "**Background**" to

--**Related Art**--.

Page 20, line 1, change "CLAIMS" to

--**WHAT IS CLAIMED IS:**--.

IN THE CLAIMS

Cancel claims 9-11, 13, 19-20 and 27 without prejudice or disclaimer.

Amend remaining claims 1-8, 12, 14-18 and 21-26 as shown below:

Sub C1

~~B2~~

1. (Amended) A method of [copy] protecting data sent from a server to a client [for presentation to a user], said method comprising:

running a program portion at the client, the program portion generating and uploading to the server a request for access to data;

cryptographically protecting the data;

sending the cryptographically protected data to the client; and

under control of the program portion, converting the cryptographically protected data to an unprotected form and selectively controlling [copying] access to copy or save functions [of] at the client in respect of the data in its unprotected [whilst the data is being held by the client in a] at form [suitable for presentation to the user].

2. (Amended) A method [according to] as in claim 1 wherein cryptographically protecting the data [is protected] comprises protecting the data by encryption.

3. (Twice Amended) A method [according to] as in claim 1 wherein cryptographically protecting the data comprises protecting the integrity of the data [is protected] cryptographically.

B2

4. (Amended) A method [according to] as in claim 3 wherein the integrity of the data is achieved by hashing.

5. (Twice Amended) A method [according to] as in claim 1 including authenticating that the client is permitted to receive the data.

6. (Twice Amended) A method [according to] as in claim 1 including identifying the client to the server before the data [is] are sent to the client.

7. (Twice Amended) A method [according to] as in claim 1 including:

generating the program portion at a server,

downloading [a] the program [object] portion to the client, and

running the program [object] portion on the client such that a request is uploaded to the server for a file containing the cryptographically protected data[, downloading the file to the client, and rendering the cryptographically protected data in an unprotected form suitable for presentation to the user,

the program object being operative such that no, or restricted, copy or save functions are offered to the user in respect of the downloaded data in its unprotected form].

8. (Amended) A method [according to] as in claim 7 [including downloading a message concerning a webpage] wherein [the message includes information concerning] the program portion is generated in response to, and corresponds with, an earlier received [object and uploading a] request for [the program object in response to said information in the message] access to the data.

12. (Twice Amended) A method [according to] as in claim 1 wherein the data [is] are sent to the client from the server through a network.

14. (Twice Amended) A method [according to] as in claim 7 wherein the program portion [object] includes data concerning a cryptographic key, and the method including using the key to render the downloaded cryptographically protected data into an unprotected form [suitable for presentation to the user].

15. (Twice Amended) A method [according to] as in claim 1 wherein the server and the client each hold data corresponding to a cryptographic key and a machine identifier for uniquely identifying the client, the method including:

sending a challenge to the client, such that it generates a signed response as a cryptographic function of the key and the machine identifier held therein,

generating from the cryptographic key and machine identifier held associated with the server, a corresponding signed response as a cryptographic function of the key and the machine identifier,

comparing the signed responses from the client and the server, and if they correspond, performing the [encryption] cryptographic protection of the data with the key, and

[performing the decryption] converting the cryptographically protected data into an unprotected form at the client with the key.

16. (Twice Amended) A method [according to] as in claim 1 wherein the data is steganographically marked.

17. (Twice Amended) A method [according to] as in claim 1 including registering the client with the server.

18. (Twice Amended) A method [according to] as in claim 1 including:

determining a machine identifier of the client by analysing its hardware and/or its software configuration,

transmitting the machine identifier to the server,

combining the transmitted machine identifier with a cryptographic key to form a unique determinator for the client, transmitting the unique determinator to the client, to be stored therein for use subsequently in identifying the client to the server, to permit encypted data to be downloaded thereto from the server.

21. (Twice Amended) A data storage medium storing [A] copy protected data [stored] on the client received by a method according to claim 1.

22. (Amended) A method of downloading encrypted data from a server to a client, said method including:

32

registering the client with the server by

determining a machine identifier of the client by analysing its hardware and/or its software configuration,

transmitting the machine identifier to the server,

combining the transmitted machine identifier with a cryptographic key to form a unique determinator for the client, and

transmitting the unique determinator to the client, to be stored therein for use subsequently in identifying the client to the server, to permit encrypted data to be downloaded thereto from the server,

subsequently identifying the client to the server on the basis of the unique determinator; and then

downloading data encrypted by means of the cryptographic key to the identified client, for decryption by the client using the key from the unique determinator.

23. (Amended) A method [according to] as in claim 22 including decrypting the downloaded data at the client using the key from the unique determinator.

24. (Twice Amended) A method [according to] as in claim 22 wherein the client is identified to the server by:

again determining the machine identifier for the client,

comparing it with the machine identifier included in said unique determinator, and

signalling to the server on the basis of the outcome of the comparison.

B2

25. (Twice Amended) A method [according to] as in claim 22 including authenticating the client to the server prior to downloading of the encrypted data.

26. (Amended) A method [according to] as in claim 25 including;

generating a challenge,

generating a response as a predetermined cryptographic function of the cryptographic key for the client as held by the server, and as a function of the key included in the unique determinator stored in the client, and

authenticating the client on the basis of the outcome of the comparison.

Add new claims 28-30:

B3 Sub B2

--28. A server for providing access to data sets in a protected form, the server comprising:

an input for receiving a request for access to a data set;

Sub D2 protecting means for cryptographically protecting the requested data set; and

generating means for generating a program portion for sending to the source of the access request,

wherein said program portion is operable, in use:

to generate a request for access to the cryptographically protected data set;

on receipt of the cryptographically protected data set, to convert it into an unprotected form; and

B3

to selectively control access to copy or save functions in respect of the data set when in said unprotected form.

Aut 71 29. A computer program carrier medium containing a computer program which implements the functions of the server in claim 28 when installed and run on a server.

Sub D3 30. A method of protecting data downloaded from a server computer to a client computer, said method comprising:

downloading a protected copy of requested data from a server to a client; and

running a program at the client to both: (a) unprotect the downloaded data thereby to provide access to an unprotected copy of the requested data, and (b) suppress client computer copy and save functions with respect to the unprotected copy of the requested data.--